A Work Project, presented as part of the requirements for the Award of a Master Degree in Finance from the NOVA – School of Business and Economics.

Operational Risk Management Framework

BNP Paribas

Opal Nassim Mabel De Souza - 27219

A DRI – Direct Research Internship Project carried out on the Master in Finance Program, under the supervision of:

Prof. Doutor Duarte Pitta Ferraz and Mr. Francisco Valério

3rd January 2018

Table of Contents

1. Acknowledgement

Firstly, I would like to express my gratitude to Prof. Duarte Pitta Ferraz, my Advisor and Professor at the Nova School of Business and Economics, for his constant support and guidance throughout the development of this project. This empirical study would not have been possible without the opportunity, experience and knowledge gained at BNP Paribas. I would like to specially thank my Manager Francisco Valério and my team Beatriz Ramalho, José Campino and Helena Bernado for their patience and guidance throughout the development of my Project. Lastly, I want to thank my parents, sister, Agnelo and Justina for their constant encouragement.

2. Abstract - Operational Risk Management Framework at BNP Paribas

The scope of this empirical study was developed within the NOVA SBE Work Project Direct Internship Programme, involving the analysis of selected processes entailed by the ORM framework at BNP Paribas. Operational Risk will constantly threaten to subvert financial institutions, hence regulators require banks to have effective Operational Risk Management (ORM) systems, so that potentially significant risks are detected and mitigated at the earliest, to safeguard stakeholders' interests (McKinsey 2016). This work project researches the relevance of the ORM model of BNP Paribas Global Markets department by examining the processes and their associated risks. By studying the operational risk trends from past incidents to identify, evaluate, and measure operational risks existence, a risk map is determined and an internal control system designed, to mitigate, evade or diminish the impact of the identified risks, thereby closing the gap to avoid similar incidents from occurring in future. Operational risk incidents highlight that standardized and structural drivers within institutions allow these events to occur and hence this empirical study elucidates that the development and implementation of an ORM framework to curtail financial impact and protect the bank's reputation is crucial and essential.

3. Abbreviations

- ORM- Operational Risk Management
- CIB- Client and Institutional Banking
- GM FO- Global Markets Front Office
- GBL- Global Business Line

4. Introduction

The stability of a financial institution is consistently threatened by a tenacious impediment called 'Risk' (ECB, 2017), which emerges in various forms including credit, liquidity, operational, market, to strongly undermine the ability of a financial institution to progress economically and for financial institutions to manoeuvre through volatile and potentially hazardous risks, development of systems and capital and liquidity buffers to provide protection against unanticipated losses is essential (BIS, 2000, ECB, 2015). In 2014, BNP Paribas, was levied a US$8.97 bn fine for deliberately masking forbidden transactions through the US financial system for entities subject to U.S. economic sanctions (Kittrie, 2016). In 2012, Barclays plc admitted to manipulating LIBOR—a benchmark interest rate that is fundamental to the operation of international financial markets and was fined US$450 mn to U.K. and U.S. regulators (HBS, 2014). In 2012 again, Standard Chartered was also fined US$340 mn by the New York State Department of Financial Services over allegations that it flouted US anti-money-laundering sanctions with Iran (Forbes, 2012). These operational risk cases in banks proved to be costly. These cases portray the need for banks to espouse practices, internal controls, behaviours, and governance mechanisms that prevent or diminish impending risks from having calamitous consequences (EBA, 2010; BIS, 2015). Due to the large size and complexity of BNP Paribas's systems, processes, regulatory environment, and nationalities, financial stability is a major concern for regulators. For this work project, I will be

addressing the gaps identified by the bank in Portugal from past incidents relating to trading and structuring teams worldwide and developing business solutions in the form of control plans to close these gaps.

5. Literature Review

The Basel Committee on Banking Supervision (BCBS) established the Basel framework after the 1970's international financial upheaval caused by the collapse of the Bretton Woods system causing several banks to shut down due to incurring cumbersome foreign currency losses (BCBS, 2015). Therefore, the central bank Governors of the Group of Ten countries established the BCBS in 1974 to enhance financial stability by improving the quality of banking supervision worldwide, and to serve as a medium for regular cooperation between its member countries on banking supervisory matters (BCBS, 2015). The BCBS is the primary global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision, and practices of banks worldwide with the purpose of enhancing financial stability. The BCBS does not possess any formal supranational authority and its decisions do not have legal force (BCBS, 2017; IFRS, 2017).

Operational risk incidents at Barings Bank, UBS and Société Générale caused enormous losses due to the illicit activities of a sole traders. However, the actual issue was inadequate management of operational risk and hence the BCBS highlights the need for banks to constantly address, the risk of losses arising due to lack of people management. (BCBS, 2001).

Nick Leeson's undetected risky trades accumulated to losses of US $1 bn ultimately causing the bankruptcy of Barings Bank due to its loosely cohering management structure and hence besides acknowledging Leeson as the sole perpetrator of the fraud, the Bank of England also emphasized on the "serious failure of controls and managerial confusion within Barings" (Hoch *et al*., 2001).

Also, the rogue trading activities of Jerome Kerviel cost Société Générale, €4.6bn in financial losses in 2008, and Kweku Adoboli cost UBS US$2.3bn in financial losses in 2011 (Gilligan, 2011). However operational risk is not subject to the actions of a sole culprit but could also occur due to comprehensive misconducts depending on the environment in which it is embedded on a daily basis (Deloitte, 2017). This is portrayed in the LIBOR manipulation scandal where mass scale duplicitous actions occurred due to a non-existent or feeble ORM systems. The lack of judicious, ethical, and transparent management systems for estimating the rates highlights a major operational risk vulnerability of the LIBOR scandal (McConnell, 2013). These cases demonstrate the impact an ineffective or non-existent ORM system has on financial institutions, thus emphasizing that it is important to implement effective ORM systems for the protection of financial institutions, and the markets, from the negative impacts by operational risk.

5.1. Operational Risk

Operational risk is defined by the BCBS as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk" (BCBS, 2001). Hence, rendering to the definition, the probable origins of operational risk are people, processes, systems, and external events. The BCBS recognizes that operational risk has a variety of meanings and therefore, for internal purposes, banks are permitted to adopt their own definitions of operational risk, provided that the minimum elements in the Committee's definition are included (Bodur, 2012). More recently, the operational risk was defined as "the risk of loss from an operational failure. It encompasses a wide range of events and actions as well as inactions, e.g., the failure to take appropriate action in a timely manner. When operational failures result in losses they are referred to as operational loss events. These losses include events ranging from unintentional execution errors, system failures and acts

of nature to conscious violations of law and regulation as well as direct and indirect acts of excessive risk taking" (Op Risk Advisory & Towers Perrin, 2010).

The term "operational risk" became prominent in recent years as it continuously evolves, occurring in different types even though, operational risk is the oldest risk faced by banks and other financial institutions (Bodur, 2012). EU legislation requires banks to adequately manage and mitigate operational risk, as it is embedded in all banking products and activities. It has always existed in banking, and other organizations but it has acquired a greater relevance given the increased complexity of products, methods and technology used in international financial markets and globalization of financial system and the recent materialization of unprecedented large losses (EBA 2016, 2017). In Portugal, banks need to establish and implement policies and procedures to assess and manage operational risk by defining the notion of operational risk, including events of reduced frequency but of great impact (BdP, 1992).

The goal of an ORM framework is identifying malfunctions and/or risks that entities are exposed to, thus preventing their occurrence, or repressing the financial implications and hence regulators require a declaration regarding all substantial operational incidents from banks, to ensure that the required capital is reserved for catastrophic operational risk scenarios (BCBS, 2011). This is illustrated in the case of Nordea, a Swedish Group that had to increase their reserve requirements substantially due to inadequate second line of defence controls, its involvement in the governance of the IRB system and modelling which also included an add-on for operational risk from inspections relating to IT and key processes (Nordea, 2015). Operational Risk is one of the important arms of the risk management triangle -the other two being Credit Risk and Market (Treasury) Risk. Any organization, particularly in the banking sector, is squarely exposed to operational risks emanating within or outside the organization. Operational Risk is also known as

Transaction Risk in some countries to efficiently face this new challenge in risk management, the prerequisites are -creation of risk culture and enterprise wide operational risk awareness. Proactive steps at all the levels of operation will operate as a safety value and in the process, may facilitate lower risk capital charge.

The BCBS demarcated seven Level 1 event types of incidents for calculating operational risk, however banks could implement an internal sub-level if necessary. (BCBS, 2002). As described by BCBS and Shevchenko in 2011 the level 1 event types are:

#	Event type	Definition
1.	Internal fraud	Losses due to acts intended to defraud, misappropriate property, or circumvent regulations, the law or company policy by an internal party
2.	External fraud	Losses due to acts of a type intended to defraud, misappropriate property, or circumvent the law by a third party
3.	Employment practices & workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events
4.	Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.
5.	Damage to physical assets	Natural disaster, terrorism, vandalism
6.	Business disruption & system failures	Losses arising from disruption of business or system failures
7.	Execution, delivery, & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors

5.2. Basel I

The BCBS developed their first framework Basel I which set 8% as the minimum capital ratio (i.e. capital to risk weighted assets) (BCBS, 2008) as the 1980s Latin American debt crisis, highlighted the necessity for safer capital ratios by consolidating capital adequacy measurements for global banking systems (BCBS, 2015).

5.3. Basel II

In 1999 Basel II, a revised version of Basel I was introduced to rectify the ambiguities identified in Basel I (BCBS, 2015), by expanding the “pillar” framework to widen the Basel Accord’s scope,

technicality, and magnitudes (Balin, 2008). Basel II is founded on three pillars: Minimum Capital Requirements, Supervisory Review, and Market Discipline (BCBS, 2004).

The minimum capital requirements pillar comprises of three components: the definition of regulatory capital, risk-weighted assets, and the minimum ratio of capital to risk-weighted assets (Balin, 2008). Banks can develop internal models for assessing their operational risk profile and determining the minimum regulatory capital requirements (BCBS, 2011).

The Supervisory review process, emphasises on the external and internal supervision of the bank's capital adequacy, (Balin, 2008), by ensuring that all past and future operational risk events are identified and understood and internal ORM systems are set up to prevent or mitigate their impact by being ethical and transparent to banking supervisors (BCBS, 2011; 2014).

Market discipline encourages disclosures from banks regarding risk exposures, capital, risk assessment processes, previously only available to regulators by publicly releasing quarterly statistics of the aggregate amounts of surplus capital held, risk-weighted capital sufficiency ratios, and credit, market, and operational risk reserves, with details of the bank's risk reduction methods (Tarullo, 2008). Basel II endowed shareholders with the ability to coerce banks to restraint their risky activities and their reserve holding approaches (Balin, 2008). Hence, if the risks taken are disproportionate to the reserves held then shareholders could penalise the bank.

Current events and criticism of Basel II have shown a profound need for a modernized Basel framework (Crisil 2017) and hence Basel III will be implemented (BCBS, 2015) in 2018.

5.4. Basel III

Basel III is a comprehensive set of reform measures, developed by the BCBS to strengthen the regulation, supervision, and risk management of the banking sector. (BCBS, 2006; 2010; 2011) These measures aim to: improve the banking sector's ability to absorb shocks arising from financial

and economic stress, (irrespective of the source), improve risk management and governance and strengthen banks' transparency and disclosures. (BCBS, 2006; 2010; 2011) The reforms target bank-level, or macroprudential, regulation, which will help raise the resilience of individual banking institutions to periods of stress and macroprudential or system wide risks that can build up across the banking sector as well as the procyclical amplification of these risks over time. (BCBS, 2006; 2010; 2011) These two approaches are complementary as greater resilience at the individual bank level reduces the risk of system wide shocks. (BCBS, 2006) (Appendix- Figure 1)

6. BNP Paribas - Corporate Profile

BNP Paribas, headquartered in Paris has service centres and operations in seventy-five countries and offers a wide range of banking and financial solutions to individuals, and commercial, corporate, and institutional clients It has more than 192,000 employees, based mainly in Belgium, France, Italy, and Luxembourg (BNP Paribas, 2015; 2016) and is considered a European leader on a global scale, due to its high brand visibility, robust brand name and reputation, that facilitates its good financial positioning. The information in the following sections have been compiled and summarized from internal procedures books of BNP Paribas and is strictly confidential.

6.1. Department Overview

The traineeship belongs to core activity: Corporate and Institutional Banking (CIB), a leader of European investment banking (BNP Paribas, 2016). CIB connects the financing needs of corporate clients with institutional clients seeking investment opportunities and is organised around 3 business lines: Corporate Banking; Global Markets; and BNP Paribas Securities Services (BNP Paribas, 2016). CIB offers tailor made financial solutions to corporate and institutional clients across capital markets, securities services, financing, treasury, and advisory solutions. It provides capital market business through the Global Markets (GM) department, comprising of seven global

business lines; Forex & Local Markets (FXLM), G10 Rates, Commodity Derivatives (CD), Primary Markets, Prime Solutions & Financing (PS&F) Equity Derivatives, and Credit. The GM department serves their clients by innovating and using efficient ways of raising and investing capital while managing the risk exposure. (Appendix- Figure 2 and Figure 3)

7. Overview of GM FO OPC & TAC Coordination Team and Process

The Operational Permanent Control and Transaction Approval Committees team in Lisbon was established in 2014 with the main goal of reducing the operational risks faced by GM Front Officers by constantly reviewing and approving processes, and creating new procedures and internal controls. Our recognized added value entails- Protection of Profit and Loss by increasing operational efficiency, supporting the different Global Business Lines (GBL) in successfully adapting to evolving regulatory landscape and ensuring smooth coordination between the GBL's, Functions and Regions. The following processes are for creating awareness, complying with governance, and reporting requirements and are in line with conduct requirements and market regulations:

1) Validation Process- The team coordinates the transactions approval and new activities committees (TAC & NAC) to ensure adherence to approval policies, business practices and relevant regulations along with supporting the Committee Chairperson. It entails performing risk assessments encountered by new transactions and activities, to ensure proper implementation of conditions by managing ad-hoc business reviews and post implementation follow ups.

   Transactions Approval Committee are exceptional transactions that are non-recurring, outstanding, often composite, or structured transactions which are not covered by the bank's risk policies or cannot assimilate to a longstanding and accepted process because of significantly unusual or

complex features and hence cannot be handled through the standard approval framework. Such transactions must be reviewed and approved through a TAC before they are concluded.

New Activity Committee are activities that cannot be initiated, monitored, or administered within the Bank's existing and written guidelines, policies, procedures or systems and hence do not fit in the current approval framework. It also includes new products and services that must be validated through a NAC before being launched.

The TAC NAC procedures provide a global framework for all business lines dealing with Capital Markets and Financing activities within the CIB departments. The validity period for a TAC approval is 3 months and 6 months for a NAC.

2) Risk & Control Assessment- The team's major responsibility is risk reduction by consistently focusing on strengthening the control system by implementing risk reduction methods and practises entailing monitoring and analysing past incidents and creating and maintaining a record of potential incidents with related action plans. The team monitors and examines recommendations made by internal and external auditors regarding business vulnerabilities identified. Risk assessments are performed at the Front officer's level with three main objectives. The first objective is Profit and Loss protection entailing identification of operational risk areas, implementing an adequate control plan, by designing and upgrading operational risk cartography in with processes, risks, and control approaches on both expected and unexpected scenarios, avoiding repetition of past incidents thereby reducing the impact on P&L, reputation, and client relationships. The second objective is monitoring and allocating regulatory capital through risk sensitive approach and satisfying the Basel requirements in terms of Advanced Measurement approach (AMA). The final objective is to demonstrate the bank's sound management of operational risk.

3) Profit & Loss protection and Risk Remediation- Focuses on strengthening the front to end control set up through the analysis of the operational risk incidents and the determination of risk reduction actions by including the respective business lines in answering, following up and closing the recommendations made by Internal governance/Audit, Regulatory, Compliance and others. Also includes participation and coordination of ad-hoc global remediation plans. Being an important procedure for identifying gaps in business level process a separate section has been dedicated to the in-depth explanation of operation risk incidents for better understanding.
4) Regulatory Governance- The team deploys and runs the Governance defined by the bank reforms and supervises specific front office processes governance along with coordinating and implementing GM & CIB regulatory initiatives.
5) Control Monitoring and FO supervision- The team oversees materializing, maintaining, and improving the FO control plans in dedicated systems, promoting of control related policies and assessment of control effectiveness and also performing controls, deploying and running a surveillance over FO's through dedicated task force.

8. Operational Risk Management Framework

The purpose of the framework is providing Senior Management with a view of the operational risk profile as per GBL's or Regions by enabling a risk based approach to be applied to the whole of GM activities and design a risk mapping based on the operational risk library. It also includes complying with AMA and non-AMA methodologies by designing Remediation Actions for all identified risk areas. The framework includes the following:

1) Risk Identification and Remediation- A Standard set of operational risk scenarios are identified and evaluated across each of the GBL's.

2) Assessment and Measurement-Operational risk is assessed across each business area to provide an aggregated GM wide view of operational risk.
3) Management and Monitoring- The operational monitoring template incorporates a risk based approach where if the severity of the risk exceeds the articulated risk appetite the bank considers enhancing the control framework.
4) Reporting and MI- Results from operational risk assessments area escalated as part of the MI packs to the senior management to ensure they have visibility over the GM Operational risk profiles
5) Reviewing and Updating- The operational risk assessment is dynamic as they are reviewed and updated on a regular basis depending on the severity of the risk scenarios identified. Risk assessments are reviewed yearly or whenever a significant change in the activity warrants it.

9. Operational Risk Cartography/ Mapping

The effort to identify and assess risks is at the heart of the permanent operational control approach; it is a dynamic process that justifies the implemented system for mitigating risk while also feeding on the information provided by this same system. The major steps of the risk mapping are:

1) The identification of the key risk areas, par event type and regulatory requirements
2) The analysis and the assessment of the underlying risks, for assessing the criticality of the main areas of intrinsic risk exposure. The underlying risk does not aim at assessing risk without any control framework, but rather the level of intrinsic risk to which an activity or a process is exposed
3) The analysis of the actual functioning of the control system is intended to assess the quality of the measures implemented for reducing the level of the underlying risk
4) The analysis of dynamic risk indicators is intended to assess the current or future distortions relative to the normal operating situation for the control system

5) The residual risk, provides an assessment of the risk having considered the actual functioning of the control framework and the results in terms of risks it gives at a given point of time
6) The underlying risk, the actual risk framework, the dynamic indicators, and the residual risk are subject to a rating that aims to synthesize the analysis.

The overall analysis process is guided by different elements that must be considered to make the rating as objective as possible. Operational risk mapping aims to recognise the pivotal areas of fundamental risks the entity is exposed to, assessing the residual risk, following the consideration of the actual permanent control framework and indicators of dynamic risk. Risk mapping facilitates a methodical approach towards operational risk management through identification, assessment, monitoring/reporting, and control/mitigation (BCBS, 2003). Risk mapping helps in formalizing and disclosing identified operational risks in a transparent manner thereby helping the bank to take corrective actions thus rectifying potential weaknesses. Appendix Figure 2

10. Operational Risk Incidents

An Operational Risk Incident is an actual event arising from the inadequacy or failure of internal processes, or from external events, which has led, may lead to a loss, gain, opportunity cost, near-miss or P&L timing. Scenarios of internal and external processes are listed below:

Failure of Internal Processes
• An internal fraud • A human error • An IT failure • Non-compliance with regulatory obligations

Failure of External Processes
• A natural disaster, accident or assault • An external fraud • Default of an external service provider • A lawsuit

A loss or gain are unexpected negative or positive impacts obtained through a failure or inadequacy of the process or arising from external events. For example, an error in the hedging a position that later exposed the position to a loss or a wrong placement of trade that later resulted in a profit.

A near-miss is an unforeseen or unplanned event that had the potential but did not cause an impact or has not occurred as the result of favourable circumstances, or was recovered within a short time of 7 calendar days. For example, an IT application was down for several minutes which could have led to a financial impact.

An opportunity cost is the benefit of the option given up when selecting a different one. Thus, in investment it is the difference between the return of the selected investment and the one passed up.

A P&L timing incident does not have any financial impact but is caused by an event that results in delayed payment or inflow of an asset.

An operational risk incident is primarily an event that must be characterized as analytically as possible, while adhering to the framework set by the Basel regulations. The Basel regulations identified seven event types, broken down on two levels. Within the BNP Paribas group, this level has been refined by adding a third qualification level that makes it possible to define a uniform set of events, thereby improving the analysis and decision capacities. (Appendix- Figure 5) An operational risk incident is defined by the "cause - event - effect" link. (Appendix- Figure 6)

Analysing the cause of an incident is an essential part of managing and preventing operational risks. A nomenclature of causes has been defined on the group level to guide the analysis and to allow for consolidations. This analysis serves to identify the entity or entities at fault, as well as the faulty process or processes. The identification of the faulty processes is mandatory for any incident higher than the collection threshold. Monitoring and reporting incidents, makes it easier to evaluate if the purpose of the ORM, to reduce the effects of the unfavourable events is being met.

It is the duty of all employees of the BNP Paribas Group to report an operational risk incident, to his/her hierarchy and the OPC team by providing clear, concise and accurate information regarding

the incident. The superior, or the employee specialized in operational risk in the team, analyses the event in compliance with the entity's rules, and declares the incident whenever necessary.

There are two main reporting tools for incidents for internal purposes- APHI and FORECAST. In APHI all operational incidents that occur globally are logged daily. If the incident results in a loss, gain, opportunity cost or near-miss above the amount of € 10k for any internal process failure or external event or € 0 for any fraud, breach of market regulation or sanction must be reported in FORECAST. Incidents reported in FORECAST are evaluated by IG, Internal and external auditors, Regulators and hence should be inserted within 3 days in cases of fraud and 10 days for other incidents which need to be closed within 6 months.

Example of hypothetical incidents reported on APHI and FORECAST:

1) IT Incident- Production database outage impacted morning trading in Asia with certain applications needing to be restarted for reconnection resulting in loss of € 20k due to loss of order priority in future rolls and late participation in Asian option market.
2) Trading Incident- Middle Office P&L team did not perform accurate checks on a registered trade to ensure that it has a flat cash position on a daily basis along with incorrect traded booked of T date which were only discovered on T+5 days and the incorrect traded where hedged with profit of € 200k. (Appendix- Figure 7 and Figure 8)

11. Recommendations

Following the identification of a failure or inefficiency of the permanent control system, by Inspection Générale, Supervisory Authority, Statutory Auditors, Management or an independent controlling function, the Management must ensure that recommendations that have been defined and validated are correctly implemented within the deadlines. In the absence of recommendations, determining whether actions are necessary and, making sure that they are correctly implemented,

in all cases, should be incorporated in the mapping of risks. These finding are analysed in the light of the (actual or potential) risk incurred and in a manner consistent with the existing risk mapping. This risk mapping must (if necessary) be updated, in terms of the underlying risk, the control system, and the residual risk.

12. Development of an Internal Control System

To protect from Operational Risk, BNPP Global Markets has implemented an Internal Control Framework based on the articulation of three lines of defence, split between Permanent & Periodic Control (Appendix- Figure 9). OPC falls within the first line of defence in which controls are generally exhaustive in nature and are required for the operational processes and risks. Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation.

The basic definition of "control" refers to "any measure taken by the management, the Board and other parties to manage the risks and increase the probability that the stated aims and objectives will be reached". A "control plan" is defined as an organized set of controls that are to be carried out and that cover all an entity's specific processes, as well as processes shared with or delegated by another entity. The OPC team oversees the designing, creation, implementation, and improvements of the control plans. The control plans should be consistent for all GBL's and regions and must conform to the practices, policies, guidelines, etc. For creating an effective control, analysing, and measuring the organization's risk exposure is essential (Scandizzo, 2005). The intensity of the control must be proportionate to the risk, and the entity's risk tolerance level. The objective of a control is to prevent a risk or to limit its impact through early detection. A control is necessarily linked to a risk, irrespective of its nature. In practical terms, the set-up of a control

results from an analysis of the risks facing the entity. The greater the risk, the greater the intensity of the control. If the risk embedded in an operation or a process is assessed as low and acceptable, the control can be limited to a self-control carried out by the person performing the operation or process. The higher the significance of the risk, the more additional controls over and above a simple self-control must be implemented, involving other employees, the management, or a dedicated team (1st level control) and/or independent permanent control functions (2nd level control). A control is considered key (or major) when it covers a major risk, i.e. the occurrence of which would have a significant effect on the results, assets, or reputation of the Group or one of its entities. The identification of the controls comprising an entity's control plan must follow a systematic analysis approach for the risks related to each process for which the entity is responsible. It should rely on a risk mapping exercise and be consistent in entities using the AMA, with the quantified potential incidents. For the system to maintain its full effectiveness, while ensuring the proper involvement of the management, the number of major controls within a generic control plan, and overall, on the entity level, must remain limited and therefore be determined very selectively.

For developing effective controls, meetings are scheduled with all teams to receive explanations regarding their processes on a deeper and more comprehensive level to recognize the potential operational risks that are posed to the bank. Once the potential risks have been analysed and mapped, internal controls are developed with the objective of bridging the gap to mitigate or possibly eliminate these risks. The following process descriptions and controls are generic examples of hypothetical teams, at BNP Paribas.

12.1. Hypothetical Trading and Structuring Teams

Trading teams offer a range of standardized products at competitive prices to both retail and institutional clients daily. Traders develop defined strategies by after deliberating over certain factors like the margins, duration of trade, payoff, the underlying, quantities and others and set specific parameters when offering new products.

Structuring teams develop customized products to address the meet the complex needs of the clients and satisfy the requirements of the bank Since structured products are tailor-made investment strategies it is imperative that they understand how to appropriately price the products created in order to handle volatility and different market environments. Below are the control plans designed specifically for each team.

Table 1: Hypothetical Trading Team's Control Plan

#	Control name	Risk Involved	Control objective	Test frequency
1	Control on Automated Trading Strategies red flags	Misexecution	Front officers must assess and escalate instances where the actual or contemplated operation of an Automated Trading Strategy has or may negatively impact a client and/or the bank, such impact has or may result in financial or reputational harm, and such harm is or may be material.	Daily
2	Control on client confidentiality	Breach of Confidentiality	Front Officers and Supervisors must acknowledge that they have personally complied with BNPP Client confidentiality guidelines, followed the Code Name Policy when communicating about flow and market color, and NOT shared information with persons who do not "need to know" such information for a valid business purpose.	Daily
3	Control on KYC and on compliance restrictions (Financial Sanction, CSR, …) against instruments / underlyings / counterparties	Failure in Client investigation (KYC, Capacity, Suitability, etc.) / Misselling	Front officers and managers ensure that they comply with the KYC Policy and with Compliance restrictions (including Restricted List, CSR Policy and Sanctions / embargoes.) Before pricing a trade, Front Officers ensure that the instrument or the underlying instrument is not on the Global Financial Security sanctions list (information available in Guard) and not on the Compliance Restricted / Black List. Before trading with a counterparty, Front Officers must check that the appropriate KYC and relevant flags are in place (in CRM Lite or CRDSweb) and that no restrictions such as financial sanctions apply to the counterparty (information available in Guard or CRMLite).	Daily
4	Control on timely trade booking	Misbooking & reconciliation failure	Front Officers and Supervisors must ensure that all trades they personnally instigated or booked are booked during their work day.	Daily
5	Control on new activities and exceptional transactions	Internal Fraud	Supervisors and/or Front Officers must ensure that all necessary approvals (including TAC / NAC and ET - Exceptional Transactions) have been obtained prior to trading or prior to starting a new activity and that all required conditions have been satisfied by their respective deadlines.	Monthly
6	Control on trader and desk mandates sign-off	Rogue Trading	Front Officers must sign off on his / her trading mandate(s), and Supervisors must sign-off on his / her desk mandate(s), on their annual anniversary and in the event of significant modification.	Annually

Table 2: Hypothetical Structuring Team's Control Plan

#	Control name	Risk Involved	Control objective	Test frequency
1	Control on Automated Trading Strategies red flags	Misexecution	Front officers must assess and escalate instances where the actual or contemplated operation of an Automated Trading Strategy has or may negatively impact a client and/or the bank, such impact has or may result in financial or reputational harm, and such harm is or may be material.	Daily
2	Control on client confidentiality	Breach of Confidentiality	Front Officers and Supervisors must acknowledge that they have personally complied with BNPP Client confidentiality guidelines, followed the Code Name Policy when communicating about flow and market colour, and NOT shared information with persons who do not "need to know" such information for a valid business purpose.	Daily
3	Control on timely trade booking	Misbooking & reconciliation failure	Front Officers and Supervisors must ensure that all trades they personally instigated or booked are booked during their work day.	Daily
4	Control on operational risk incident escalation	Internal Fraud	Front Officers and Supervisors must ensure that any operational risk incident they are aware of has been properly reported to their Manager and to the GM OPC team and that appropriate actions have been taken.	Weekly
5	Control on new activities and exceptional transactions	Internal Fraud	Supervisors and/or Front Officers must ensure that all necessary approvals (including TAC / NAC and ET - Exceptional Transactions) have been obtained prior to trading or prior to starting a new activity and that all required conditions have been satisfied by their respective deadlines.	Monthly
6	Control on trader and desk mandates sign-off	Rogue Trading	Front Officers must sign off on his / her trading mandate(s), and Supervisors must sign-off on his / her desk mandate(s), on their annual anniversary and in the event of significant modification.	Annually

13. Control Monitoring and Front Officer Supervision

ARIS Architect & Business Designer (ABD), is an internal tool used for creating, managing, analysing, and administering the control plan models of front officers and their teams. After completing the modelling in ABD, the control plans are then imported onto the application ARCM (ARIS Risk and Compliance Manager), commonly called ORUS FO. ARCM is an application used by front officers for viewing and validating their controls, or reporting any operational risks encountered while executing their daily tasks. ARCM also allows for a two- way communication between Front Officers and OPC team, where the OPC can inform the Front Officer of any potential risks arising due to incompletion of certain tasks through the specific controls and the comment sent by the OPC team is called "Pre-assessment". A "Pre-assessment" risk level is inserted by selecting either the red, orange, or green colour to signify that the risk of not performing the task is high, medium, or low respectively. This helps in early detection and aversion of potential operational risks. Thus, ARCM plays a significant role in effectively managing, controlling, and mitigating potential risks.

14. Conclusion

Within the NOVA Work Project Direct Internship Programme, the scope of this empirical study, involved performance of an internal analysis of the processes performed by the BNP Paribas Global Markets Front Office team to infer the effectiveness of having a robust operational risk management framework. Prominent operational risk incidents, like the rogue trading activities at Barings Bank, Société Générale, UBS, and lack of controls at Nordea, highlight the severe financial impacts caused by not implementing robust, effective, and efficient ORM frameworks. In hindsight, early identification of these incidents could have significantly reduced the financial impact to the minimum or could have possibly been negligible. Thus, drawing attention to the

existence of standardized and structural drivers within the organisation's environment that caused their insolvency.

These leads to the conclusion that, misconducts are not isolated events occurring due the sole activities of an individual with a financial institution. As demonstrated by the LIBOR scandal, the origins may initially be trivial but can intensify to cause a global financial crisis due to unethical ways of conducting business. This empirical work concludes that, robust, and effective ORM systems are vital in helping financial institutions in depicting the probable impacts of identified operational risks but also in preventing the massive negative impacts through spillage into the financial markets.

To conclude the establishment of a first line of defence that is both systematic and effective is of vital importance for the early detection of potential risks and subsequent mitigation or avoidance of its impact on financial institutions. As a result, to protect the financial, reputational, and/or operational stability from the negative impacts of unfavourable and unanticipated events defensive measures need to be taken against possible risks.

A complete risk-free environment is difficult to achieve, therefore developing and implementing a customized and comprehensive ORM framework should be of vital importance to all financial institutions. Therefore, the Work Project's research process focuses on BNP Paribas' development of a risk cartography, designing and implementing of internal control systems to combat the potential risks.

This empirical study has meaningful contributions to the literature and the business world, since to the best of our knowledge this work project provides a thorough insight into BNP Paribas' ORM systems. This work project provides a unique and insightful elucidation on the internal processes

of developing control plans through risk mapping and a concise view of implementing these control plans through internal system.

Due to confidentiality reasons, the main limitation of this research was caused by the restrictions on sensitive information and internal data, thus a more detailed insight could not be providing that would further enrich the study. Another consideration for further research could the one that explores into the quantitative characteristics of ORM with the help of the bank's internal data. Furthermore, the implementation of Basel III, would demand changed in the ORM framework and thus, it would be interesting if the following researches would highlight the effect these changes would have on the new qualitative and quantitative aspects in preventing operational risk incidents.

References

Balin, B. J. (2008). *"Basel I, Basel II, and Emerging Markets: A Nontechnical Analysis."* The John Hopkins School of Advanced International Studies.

Banco de Portugal. (1992). *"Regime Geral das Instituições de Crédito e Sociedades Financeiras"* Artigo 115.º-T Risco operacional.

Bank for International Settlement. (2015). *"85th Annual Report."*

Basel Committee on Banking Supervision. (2001). *"Consultative Document: Operational Risk."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2002). *"Operational Risk Data Collection Exercise."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2003). *"Operational risk transfer across financial sectors."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2003). *"Sound Practices for the Management and Supervision of Operational Risk."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2006). "*International Convergence of Capital Measurement and Capital Standards."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2006). *"International Convergence of Capital Measurement and Capital Standards."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2008). *"Part 2: The First Pillar – Minimum Capital Requirements."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2010). *"Basel III: A global regulatory framework for more resilient banks and banking systems."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2011). *"Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2011). *"Principles for the Sound Management of Operational Risk."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2014). *"Review of the Principles for the Sound Management of Operational Risk."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2015). *"A brief history of the Basel Committee."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2016). *"The Basel Committee Charter."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2017). *"Basel III: Finalising post-crisis reforms."* Bank for international Settlement (BIS).

Basel Committee on Banking Supervision. (2017). *"The Basel Committee mandate."* Bank for international Settlement (BIS).

BNP Paribas (2015), *"Annual Report 2015."*

BNP Paribas (2016), *"Report on Activity and Corporate Responsibility 2016."*

BNP Paribas (2017), *Internal Procedures Books*

Bodur, Zülal. (2012). *"Operational Risk and Operational Risk Related Banking Scandals/ Large Incidents."*

Centre for Regulatory Strategy. (2017). *"Managing Conduct Risk."* Deloitte Touche Tohmatsu Limited.

Committee of European Banking Supervisors. (2010). *"Guidelines on the management of operational risks in market-related activities."* European Banking Authority (EBA).

Constâncio, Vítor. (2015). *"Financial stability risks, monetary policy and the need for macro-prudential policy."* European Central Bank.

Crisil. (2017). "Basel III liquidity risk: The implications."

Cruz, Marcelo G, and Peters, Gareth W. and Shevchenko, Pavel V. (2011), *"OpRisk Data and Governance."* Fundamental Aspects of Operational Risk and Insurance Analytics: A

Handbook of Operational Risk. Wiley Publications.

European Banking Authority. (2015). *"Joint Committee of the European Supervisory Authorities Report on Risks and Vulnerabilities in the EU Financial System."*

European Banking Authority. (2016). *"The EBA 2017 Work Programme."*

European Banking Authority. (2017). *"The EBA 2018 Work Programme."*

European Central Bank. (2017). *"Financial Stability Review."*

European Central Bank. (2017). "*Financial Stability Review*".

Gilligan, George. (2011), *"Jérôme Kerviel the 'Rogue Trader' of Société Générale: Bad Luck, Bad Apple, Bad Tree or Bad Orchard?"* The Company Lawyer, Vol. 32, No. 12.

Hoch, Stephen J, Kunreuther Howard C, and Gunther, Robert E. (2004). *"Chapter 1: A Complex Web of Decisions."* Wharton on Making Decisions. Wiley.

International Financial Reporting Standards (IFRS). (2017). *"Basel Committee on Banking Supervision and IFRS Foundation Sign Memorandum of Understanding."*

Kaminski, Mikkelsen, Poppensieker, and Raufuß. (2016). "*Nonfinancial risk: A growing challenge for bank*." McKinsey & Company.

Kittrie, Orde F. (2016). *"Lawfare: Law as a Weapon of War."* Oxford University Press

McConnell, Patrick. (2013). *"Systematic Operational Risk: The LIBOR Manipulation Scandal."* Journal of Operational Risk.

Mercedes, Siury M. (2016). "Implementing an Operational Risk Management Framework at BNP Paribas Lisbon: A Case Study."

Meyer, Laurence H. (2000). *"Why risk management is important for global financial institutions?"* Bank for International Settlement (BIS).

Nordea Press Release. (2015). *"Comment on the Swedish Financial Supervisory Authority's decision of 18 May 2015."*

Op Risk Advisory & Towers Perrin. (2010). *"A New Approach for Managing Operational*

Risk: Addressing the Issues Underlying the 2008 Global Financial Crisis."

Rose, Clayton S and Sesia, Aldo. (2013; 2014). *"Barclays and the LIBOR Scandal."* Harvard Business School.

Scandizzo, Sergio. (2005*). "Risk mapping and key risk indicators in operational risk management."* Economic Notes.

Tarullo, Daniel. K. (2008). "*Basel I." Banking on Basel: The Future of International Financial Regulation."* Peterson Institute for International Economics.

Touryalai, Halah. (2012). *"Standard Chartered Will Pay Another $327M For Illegal Iran Dealings."* Forbes.